## Networks And Communications

*Networks and Communications in 2020 enable Battle Command; guaranteed communications allows the commander to command. The network, which is the major enabling component of the Global Information Grid, provides assured, secure, worldwide network access that is ubiquitous, autonomous, and reliably supports all required tactical, operational, and strategic needs. It is joint and transparently interoperable with interagency organizations and multinational allies. Network and Communication systems with their core essential services and Community of Interest services provide warfighters with proactive, intelligent, decision-oriented, and knowledge-enabled capabilities. Staff planning and functional management are now distributed and decentralized, reducing the footprint in an area of operations to the essential warfighting assets.*

In 2020 the network is intelligent; it automates much of the routine planning work, such as course of action analysis, fire selection, collection management, logistics, and bandwidth management, allowing the commander to focus on the art of command. The network, always on and always available, proactively plans and coordinates in support of the commander and the mission. These assured communications family of services enable near perfect situational awareness and, in conjunction with persistent surveillance and a complete operational picture, have dramatically changed how we fight. This new way of war has so impacted the fight that we typically overwhelm an enemy before they know the battle has been joined. The network enables precise maneuver, fires, and sustainment; we never have meeting engagements and swarm an enemy relentlessly.

Networks and Communications support the full range of battle command functions: battlespace awareness, command and control, sustainment, medical, human resources, deployment, readiness, etc. Network and Communication systems are now intelligent to the point that they proactively provide connectivity and knowledge to leaders and managers, from strategic levels, through operational, to tactical. Joint business practices are now ingrained into the network fabric as knowledge-enabled services, accessed by anyone with a valid need, reliably, from anywhere in the world at any time. Stovepipe, stand-alone systems no longer exist. Now, entire business functions and processes have been converted into net-centric services available whenever and wherever needed. Advanced biometrics recognize users, grant their access authorization, and authenticate them into the network, providing worldwide access to job and mission resources. Networks and Communications with knowledge–based enterprise services enable all the joint warfighting and functional domains.

The signal force has been significantly restructured as a result of the vast increase in autonomous operations. Signal forces, as well as information operations forces; intelligence, surveillance, and reconnaissance (ISR) forces; and space forces are now consolidated into the joint U. S. Information Operations Command. Soldiers of all specialties receive training in network tactics and techniques, in particular to attain proficiency in the dynamics of their integrated platforms.

There are three key focus areas to Networks and Communications: Net-Centric Operations, Knowledge Operations, and Network Operations.

**Net-Centric Operations**

*Networks and Communications are a component of the Global Information Grid (GIG); they are inherently integrated with joint, interagency, and multinational systems and enable worldwide operations. The single information network serves all users and uses. Integrated communication systems are embedded into every platform, making every platform a Network and Communication device.*

The physical infrastructure of the network creates an umbrella-like coverage over our worldwide operational area. Communication systems no longer "reach back" or "reach," they simply connect. This gives commanders, staffs, and business process managers the "always on" connectivity required for battle command. Enterprise architectures enable the network.

Networks and Communications form the basis for the GIG. This means the Army cannot provide communications without the joint components of the GIG; we rely on it being available and operational. Likewise, the GIG is dependent on the Army's networks and communications being available and operational. This symbiotic relationship characterizes network and communication services in the 21st century.

Networks and Communications are transparently joint. They interoperate virtually without gaps or seams among interagency organizations and multinational allies. The network is self-organizing and self-configuring. It is multi-layered, composed of terrestrial, air, and space based systems, forming a network of networks. Terrestrial and airborne systems use both opportunistic and dedicated communication packages. Airborne and space-based communication assets provide coverage over wide areas and into communications-restrictive terrain. Software defined radio systems operate in multiple frequency bands, offer high throughput, and employ conformal antenna technology and capabilities to automatically convert from omni-directional to uni-directional operation. Self-forming networks enable communications-on-the-move and operational maneuver from strategic distances. Automatic cross-linking, cross-banding, background routing, and highly intelligent network decision management systems create the fully meshed network structure. Autonomous network operations are transparent to the ground force commander.

Network and Communication devices no longer exist as separate components; they are tightly embedded into all platforms. A personal user interface provides all voice, video, text, and data input and output. Voice commands have replaced the need to know phone numbers, e-mail addresses, net frequencies, or call signs.

Network knowledge systems support the full range of operational and business requirements, which include, for example, functional business management, home

station operations, training, mobilization, deployment, employment, and redeployment. Tactical units are able to receive updates, conduct collaborative en route mission planning and rehearsals, create a tailored common operational picture (COP), and gain situational understanding, all leading to decisive action.

This encompassing network connectivity has reduced all units' in-theater support footprint. The advantage of advanced and reliable technology is that the physical location of support and administrative staffs is no longer important. Real-time situational understanding enables remote, decentralized staff operations.

**Knowledge Operations**

*The information systems now available, joint by design, have a degree of intelligence not seen before. These systems know who you are, what organization you belong to, what you do, where you are, your security requirements, and, therefore, understand what you need to know – the knowledge you need to perform your job or mission. Because of this, information systems have automated a large portion of the decision-making process. These systems proactively provide knowledge as or before it is needed.*

Knowledge systems compress decision time by providing real-time connectivity and computing power for warfighters, national security users, and business process managers. These systems give leaders the ability to make knowledge-enabled decisions. Rapid exploitation of diverse data sources by individual and organizational users allows customization of knowledge to meet specific mission demands. The Infostructure – the combined structure of information within the net-centric framework – is intelligent and proactive across the entire spectrum of operations. It understands the knowledge needs of commanders, staffs, and business managers. The underlying knowledge requirements that drive the system are derived from commander's intent, priority information requirements, METT-T, organizational policy, and situation-unique requirements.

Current enterprise knowledge applications have greatly increased the effectiveness of commanders, staffs, and business process managers. These applications include powerful search and analysis engines, robust information cataloging, content dissemination based on profiles and relevant context, and predictive decision aids. Planning and decision support tools assist users at every echelon in the decision making process. The system, among other things, does mission and job analysis, course of action (COA) analysis, recommends actions, and generates task lists. Within set conditions or parameters, the applications make autonomous decisions. Virtual collaborative staffing allows participation by special staffs, engineering expertise, and other external elements not commonly associated with the unit or organization. Parallel planning methodologies link multiple echelons into simultaneous planning cycles.

The knowledge systems are learning enabled: a user's continued interaction with the system causes it to learn about the user and anticipate future needs. There is little system configuration required by the user other than setting general parameters at the beginning of an operation or training event.

**Network Operations**

*Network Operations (NETOPS) is a set of critical enterprise functions that provide network management, information dissemination management, and information assurance. It increases the efficiency and effectiveness of system operation, provides dynamic bandwidth and spectrum management, and keeps the network operational. The Networks and Communications system of systems, including NETOPS, is highly automated, with little operator intervention required. NETOPS is a joint and interagency function in which the Army participates.*

Network Operations keep "the pipes open." Because of NETOPS, users are assured that the network is always available to support their dynamic needs.

The automated network management system, with operator intervention as required, monitors, configures and controls all aspects of the network transparently to warfighters and institutional users. NETOPS functions are largely performed from strategic locations. NETOPS manages the networks and provides a robust defense-in-depth that detects, reacts, and responds to attacks on our networks. The unprecedented level of connectivity introduces the possibility of new vulnerabilities and increases the potential of significant damage if our networks are breached. However, our networks are nearly impenetrable because of the network protection mechanisms designed in and because we are now fully integrated with the offensive and defensive aspects of Information Operations (IO).

Adversaries continue to attack our systems with advanced intercept, jamming, network attacks, and other capabilities, but our systems are flexible, able to adapt, and have achieved a low probability of intercept and detection. Encryption is ubiquitous and simple to use, to the point that it is completely hands-off to the user. Users no longer load communications security keying material or perform similar functions. The network loads and keys itself. Encryption is on all communication links; plaintext is never used except to communicate with 20$^{th}$ Century-era forces. Personal identification and authentication is now done with 100% guaranteed, reliable, assured biometrics. True multi-level security has been achieved, further simplifying the structure of the network and command operations using the network. The mechanisms and procedures for disseminating and sharing classified information with interagency and multinational organizations have been established and are in place. Systems are protected against environmental hazards, to include electromagnetic pulse.

The network is self-maintaining and self-healing. Automated NETOPS processes recognize when there is a deficiency, degradation, or outage and apply corrective action automatically up to the point of physical hardware replacement. When

needed, the network autonomously launches Unmanned Aerial Vehicles (UAVs) or re-directs UAV resources to provide communication services. The flexible, redundant connectivity and self-healing properties of the network, along with real-time network management and network defense, reduces the vulnerability of our information systems and improves their ability to survive. Network-centric systems no longer contain single points of failure. The layered, redundant components, in conjunction with robust NETOPS capabilities, means the chance of a soldier being out of communications range is very unlikely.

While the electromagnetic "battlespace" remains a challenge, it has also become easier to manage. The frequency spectrum, as an internationally recognized, shared asset, continues to become more crowded and less accessible. However, adaptive networks and dynamic, opportunistic management and allocation of spectrum have made our networks more efficient and effective. Automated systems allow us to perform frequency management from strategic locations. Operators no longer set frequencies or load hop-sets; these are automatically propagated throughout the network. Bandwidth allocation is automated based on mission and commander requirements. Information systems have been carefully designed to minimize their bandwidth requirements.

*Advanced Network and Communication capabilities and knowledge-enhanced processes enable the art and science of battle command. It allows warriors to gain decision dominance over and take decisive action against all adversaries. The Army acts jointly with power and precision never before seen on the battlefield.*